

---

# **Gli attacchi cyber in Italia e nel mondo: i dati Clusit a confronto**



# Gabriele Faggioli

**Responsabile Scientifico Osservatorio Cybersecurity e Data Protection  
Politecnico di Milano**

**Presidente CLUSIT (Associazione Italiana per la Sicurezza Informatica)**

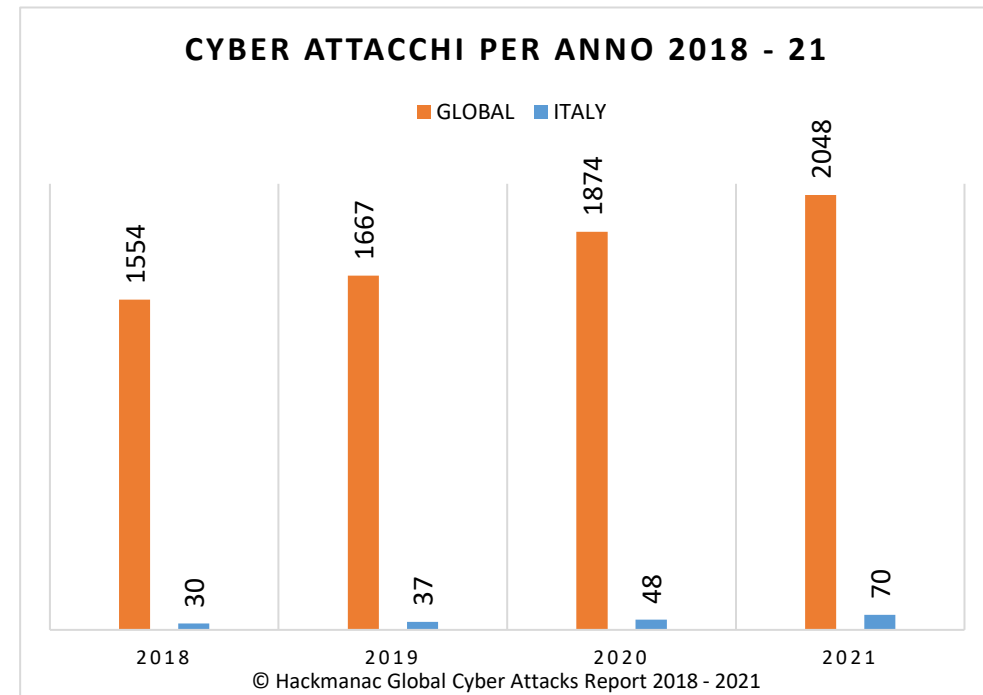
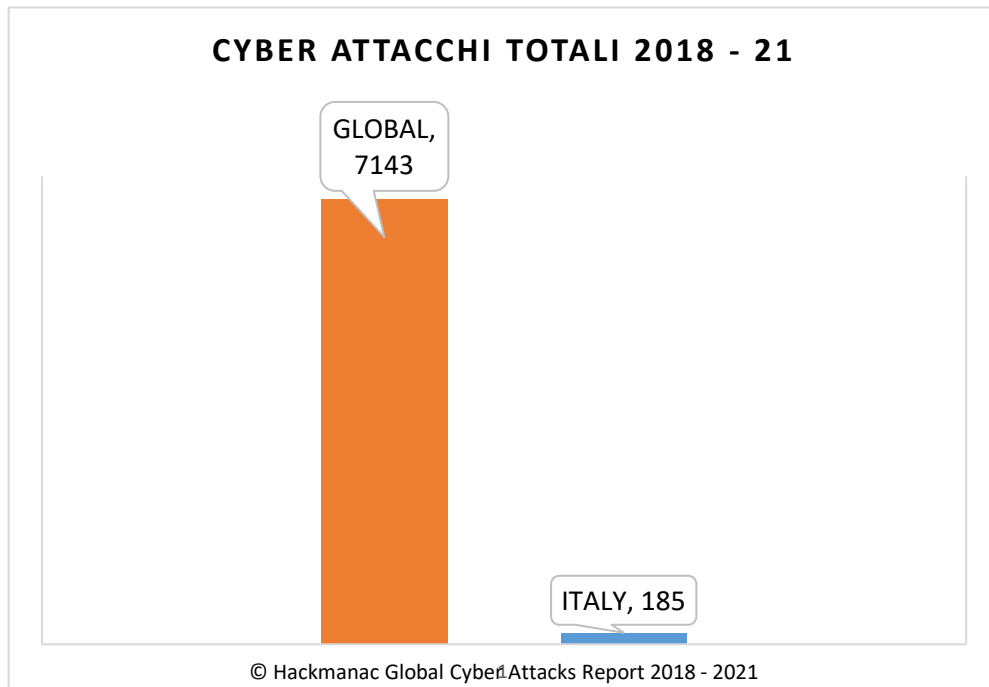
**Adjunt Professor MIP-Politecnico di Milano**

**Professore a Contratto in Diritto del management delle ICT  
Economia & Commercio Università di Pavia**

**CEO Digital360 – Partners4innovation**

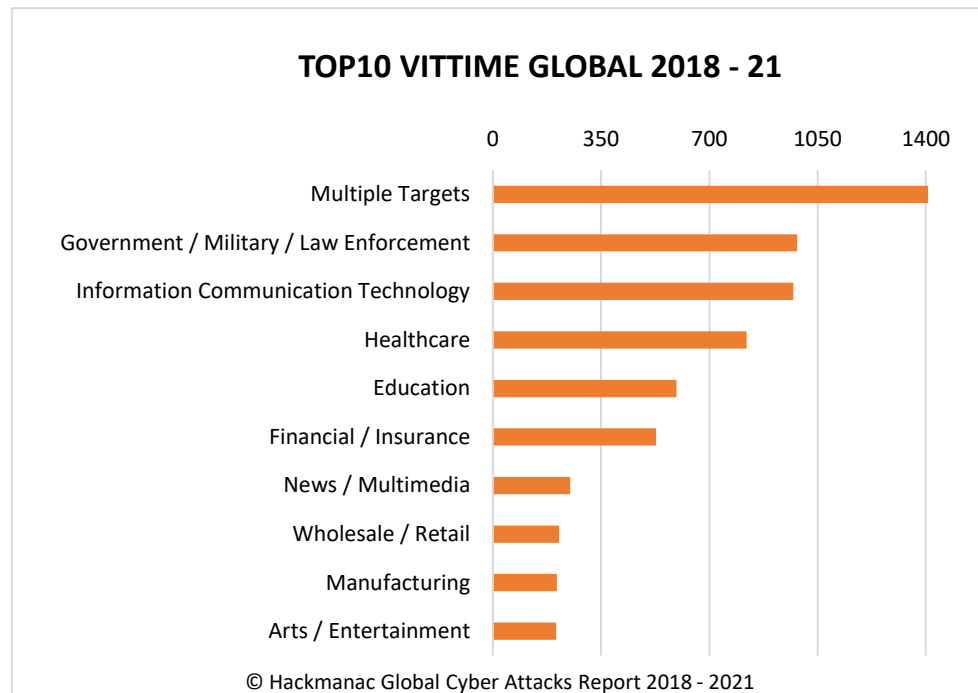
**[faggioli@mip.polimi.it](mailto:faggioli@mip.polimi.it)**

# Gli attacchi cyber aumentano nel mondo e in Italia



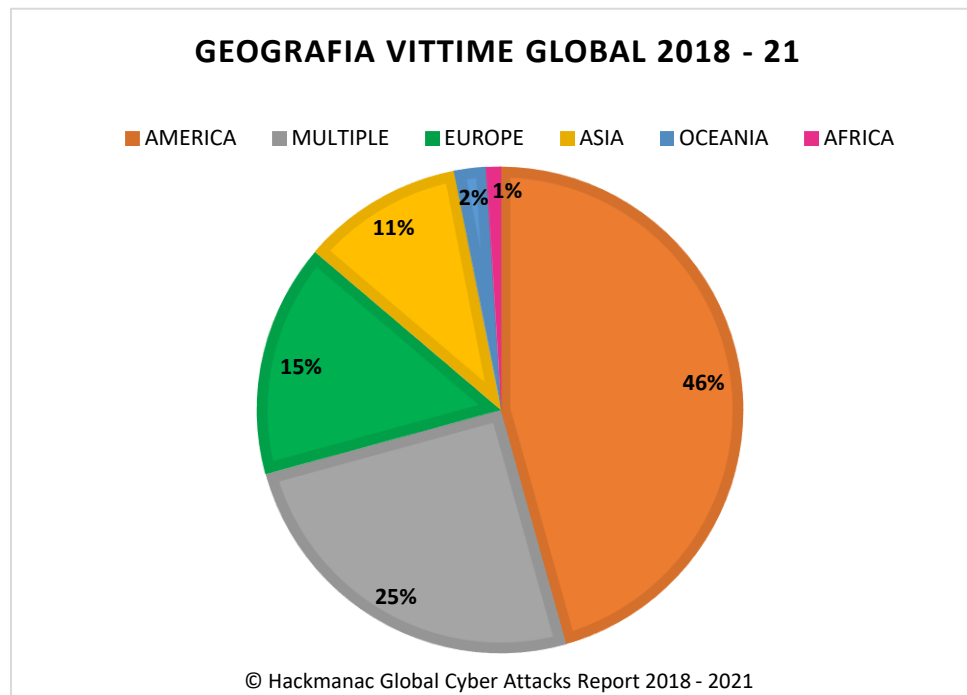
Nel periodo 2018 - 2021, sono stati censiti 7.143 cyber attacchi a livello globale, di cui 185 in Italia. Gli attacchi cyber verso realtà basate in Italia sono più che raddoppiati, da 30 a 70, a fronte di un aumento globale dai 1.554 attacchi rilevati nel 2018 ai 2.048 del 2021.

# Sanità e PA tra le organizzazioni più colpite



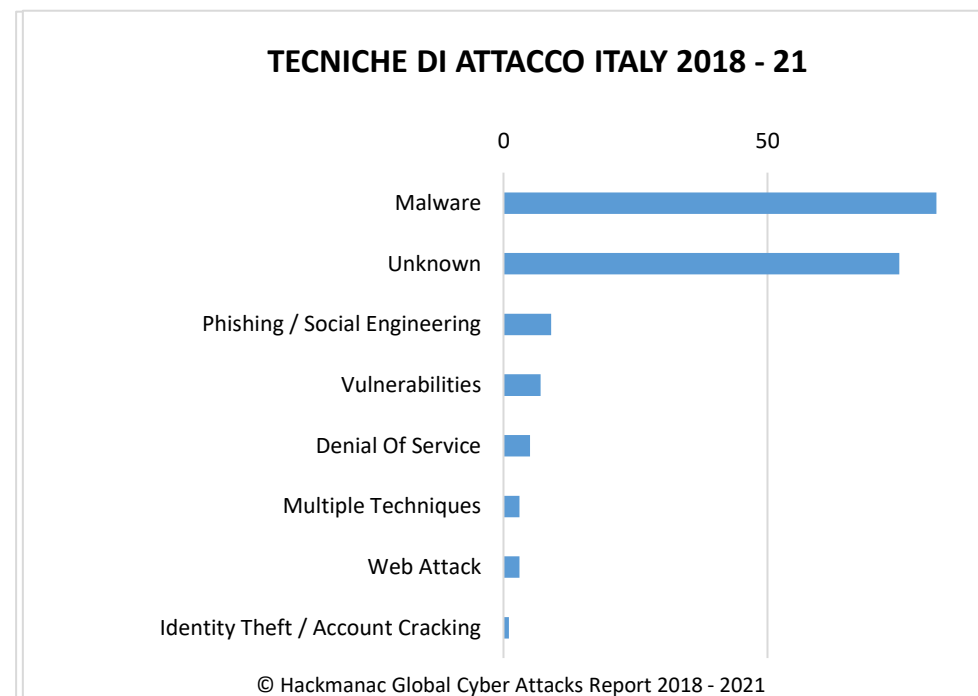
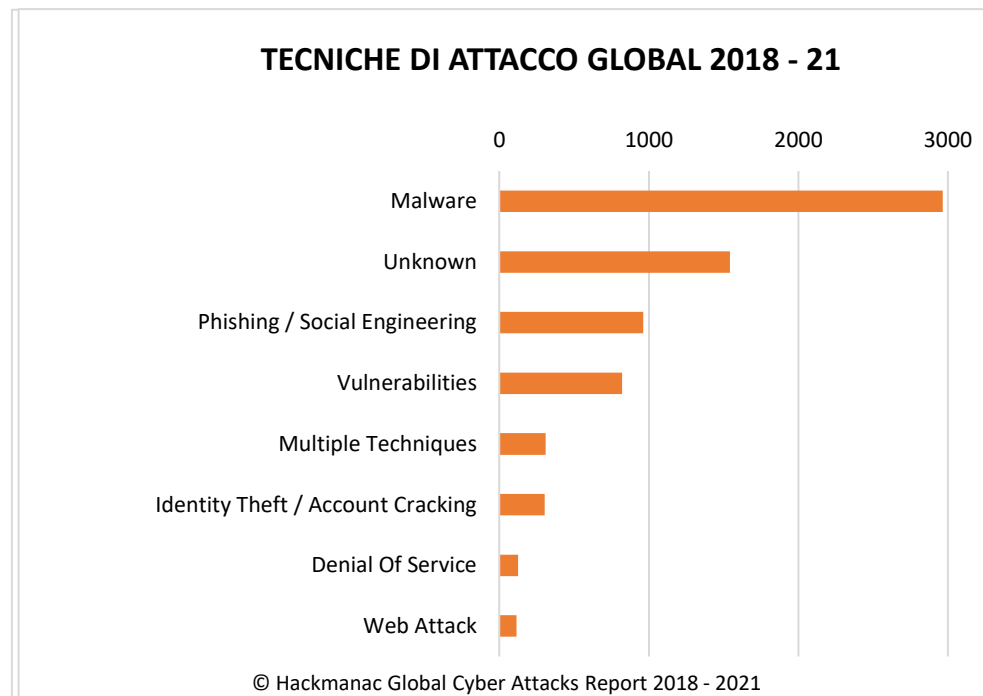
- La quota più significativa degli attacchi rilevati a livello globale (quasi il 20%) prende di mira bersagli multipli. Al secondo e terzo posto tra i settori più colpiti vi sono le categorie Government / Military / Law Enforcement e Information Communication Technology, ciascuna con circa il 13% del totale.
- In Italia, la categoria più colpita è quella Government / Military / Law Enforcement, oggetto del 27% degli attacchi censiti. Seguono le categorie Manufacturing e Healthcare con, rispettivamente, il 13% e il 10%.

# Europa la seconda regione più colpita



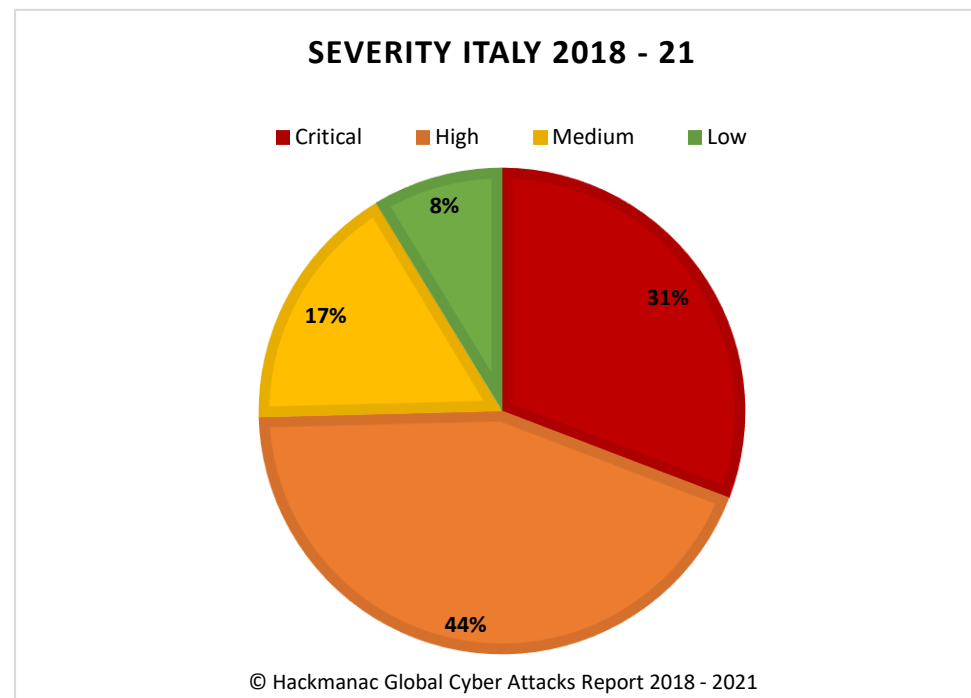
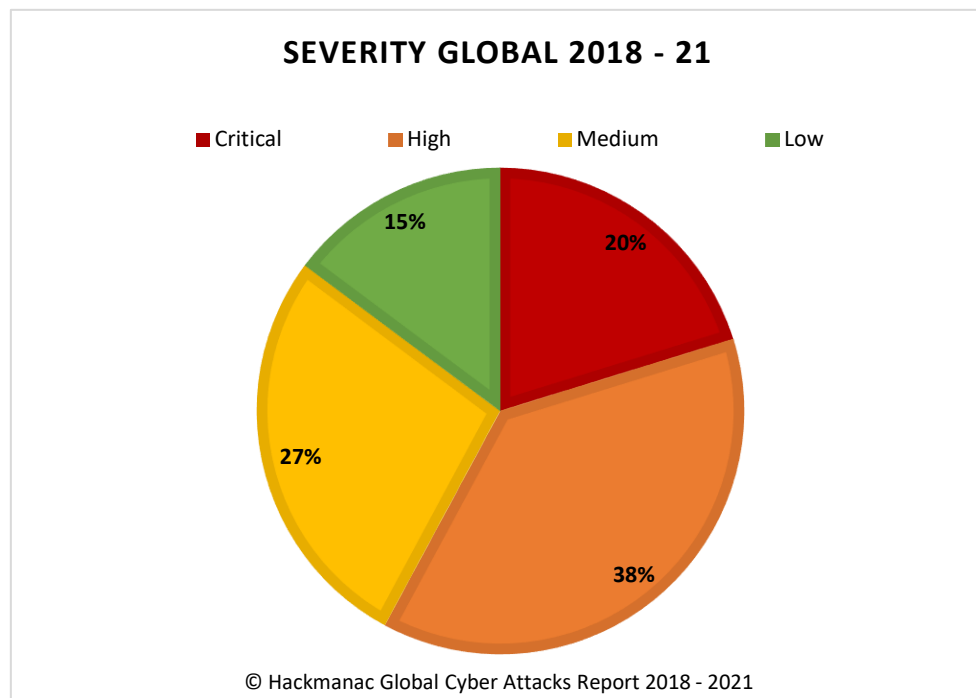
La regione maggiormente afflitta dagli attacchi cyber è l'America, con il 46% degli attacchi censiti. La seconda quota più rilevante, pari al 25%, riguarda vittime riconducibili a più regioni, mentre l'Europa si posiziona al terzo posto di questa classifica, con il 15% degli attacchi.

# Malware e social engineering ancora predominanti



Sia a livello globale che in Italia, la tecnica di attacco più utilizzata è il Malware, riconducibile, rispettivamente, al 42% e al 44% degli attacchi. La categoria Malware precede quella Unknown, con il 22% degli attacchi a livello globale e il 41% di quelli a livello italiano. Al terzo posto troviamo la categoria Phishing / Social engineering, a cui si riferisce il 13% degli attacchi a livello mondiale e il 5% di quelli a realtà italiane. La categoria Unknown rappresenta attacchi per i quali non si è riusciti a risalire alla tecnica utilizzata.

# In Italia, 3 attacchi su 4 hanno impatti elevati o critici



Il 20% degli attacchi rilevati tra il 2018 e il 2021 a livello globale ha avuto un livello di severity «Critical». In Italia, la percentuale di attacchi «Critical» sale al 31% del totale.

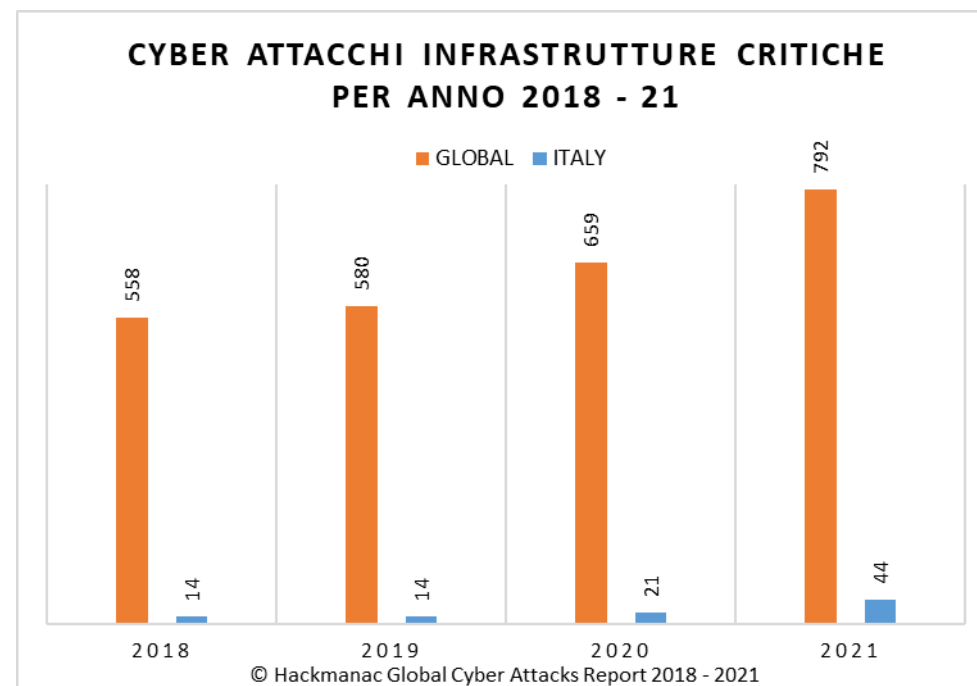
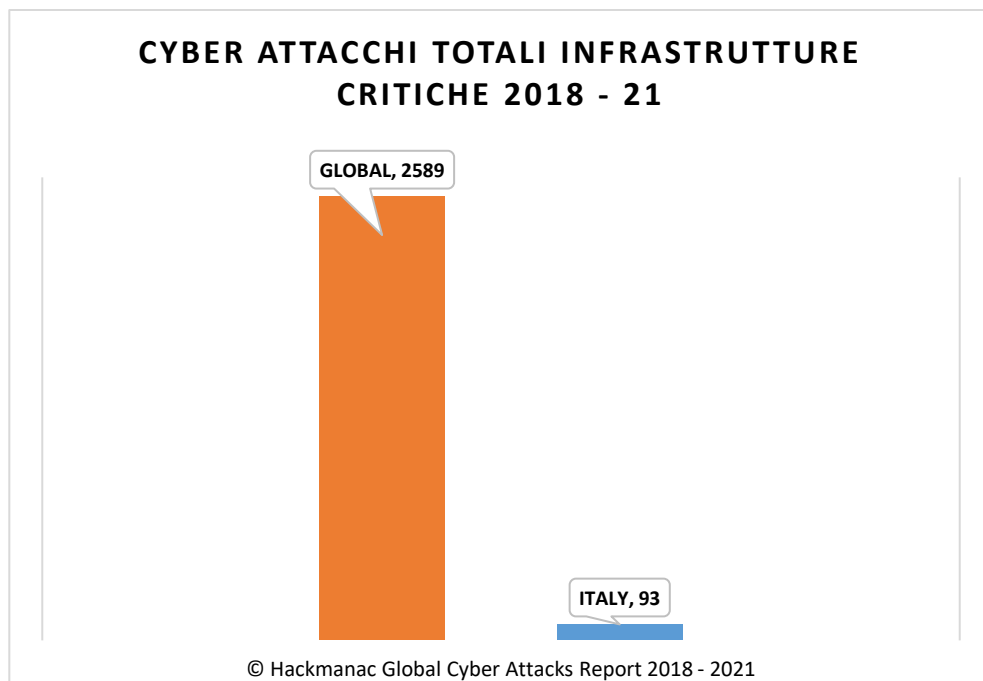
Per severity «Critical» si intendono attacchi rivolti a settori critici o comunque aventi impatti molto gravi, con perdite economiche rilevanti (nell'ordine dei milioni di euro) o altre ripercussioni di entità molto significativa.

---

# **Gli attacchi alle infrastrutture critiche**

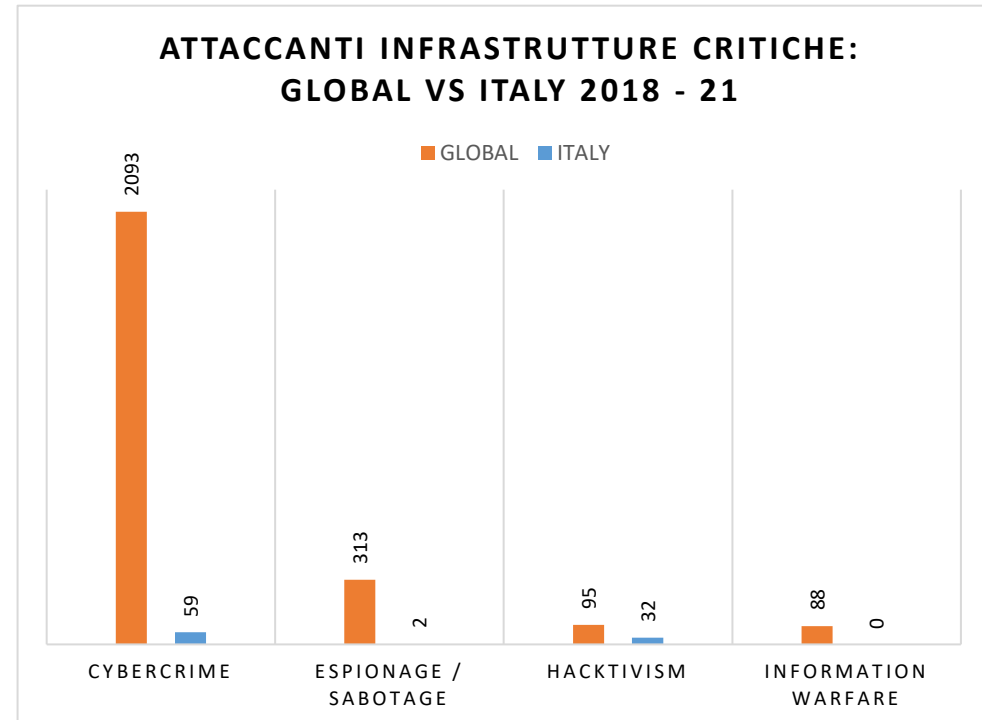


# Aumentano gli attacchi alle infrastrutture critiche



Nel periodo 2018-2021 sono stati censiti 2.589 cyber attacchi a infrastrutture critiche a livello globale e 93 a livello italiano. A livello globale, gli attacchi alle infrastrutture critiche rappresentano circa il 36% del totale, mentre in Italia tale quota è di poco superiore all'1%.

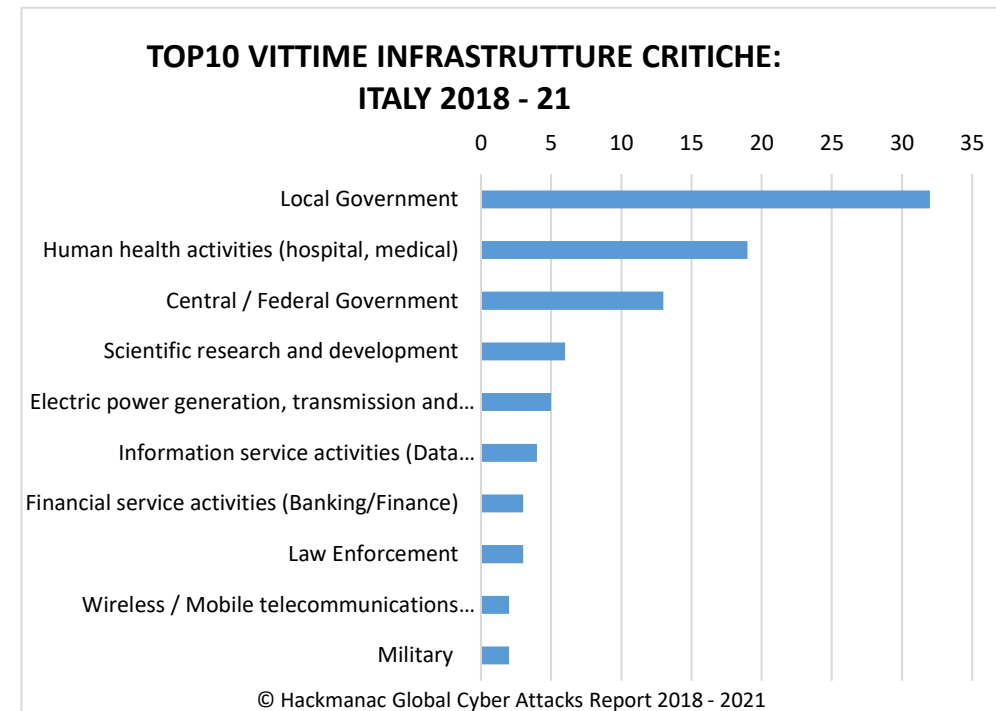
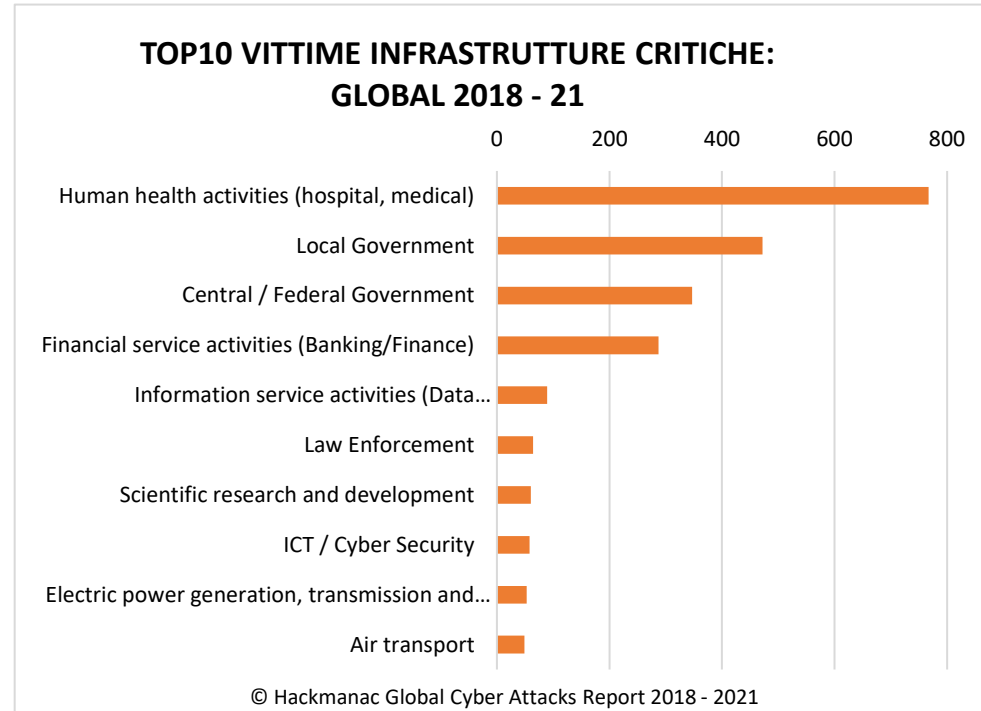
# Cybercrime principale minaccia anche per le infrastrutture critiche italiane



© Hackmanac Global Cyber Attacks Report 2018 - 2021

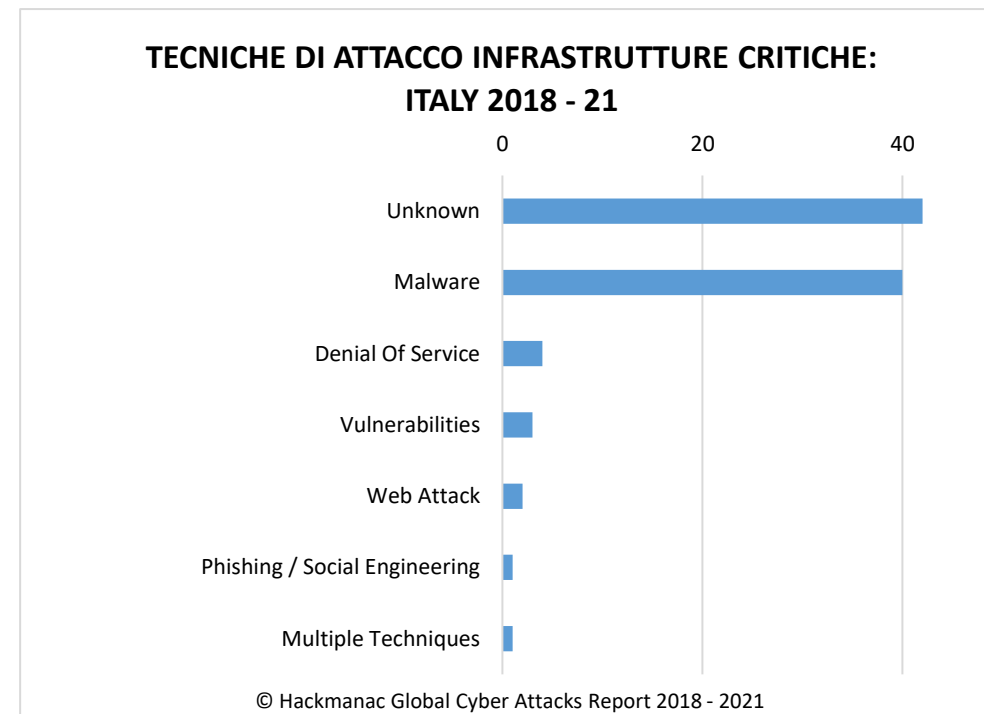
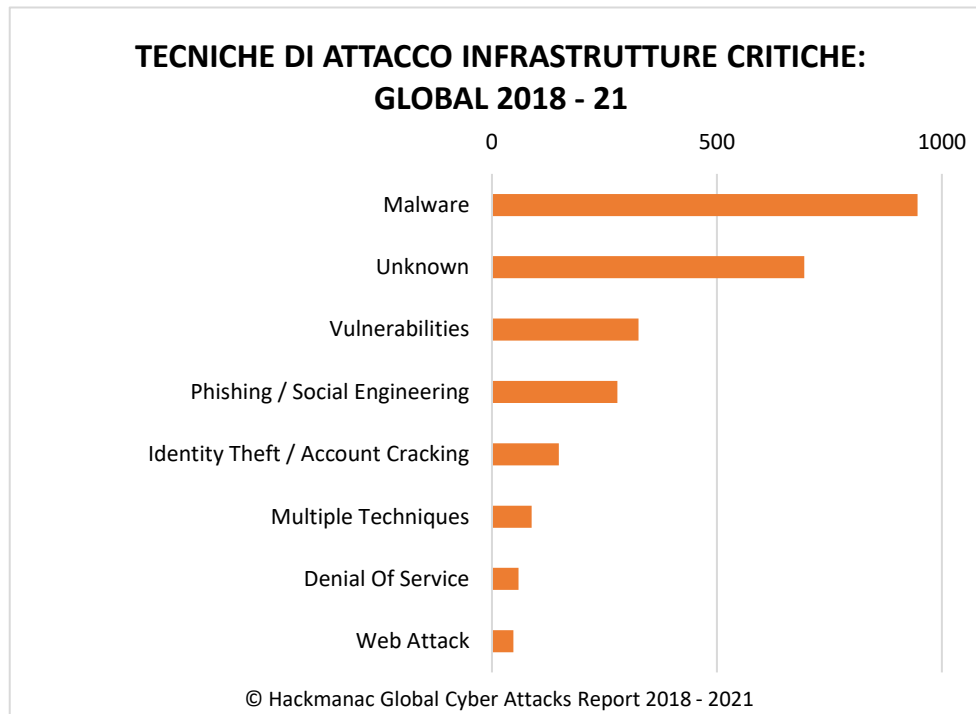
Sia a livello globale che in Italia, il Cybercrime rappresenta la principale fonte di attacchi alle infrastrutture critiche: nel triennio 2018-2021 sono stati rilevati 2.589 attacchi Cybercrime ad infrastrutture critiche a livello globale, a fronte di 93 casi afferenti a realtà italiane.

# Sanità e PA i settori più colpiti



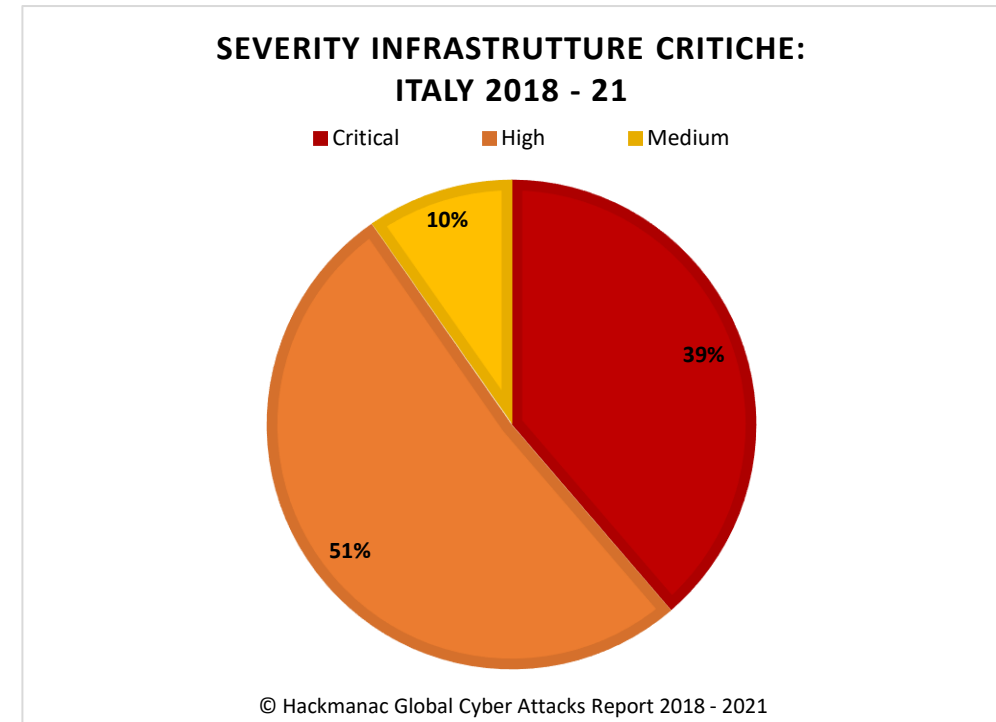
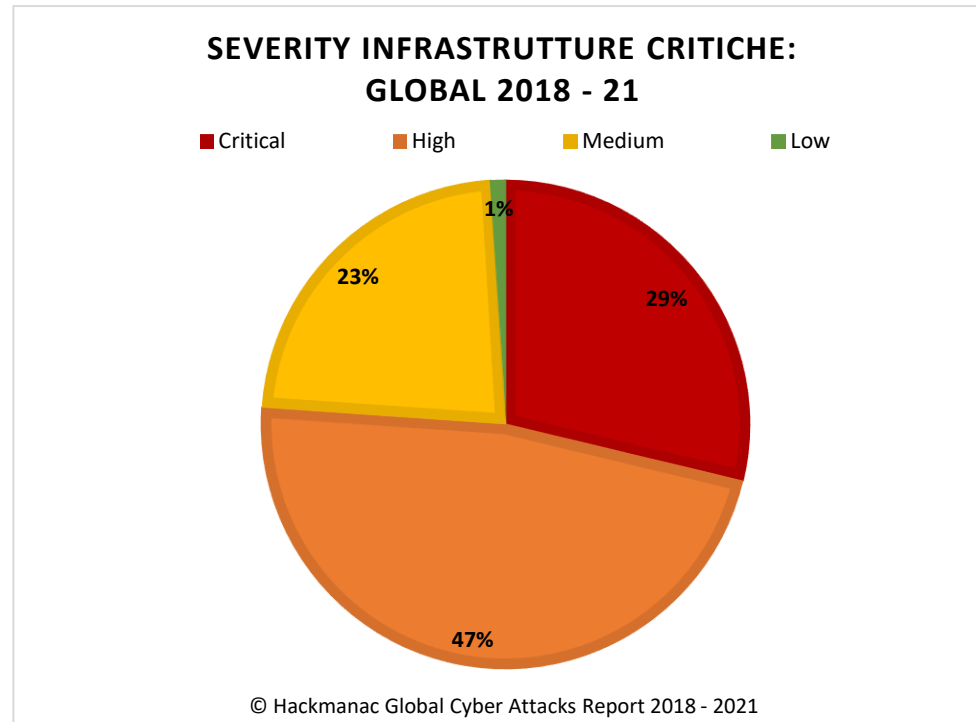
Per quanto riguarda gli attacchi alle infrastrutture critiche, le organizzazioni più colpite a livello globale appartengono ai settori Human health activities, Local Government e Central / Federal Government, rispettivamente, con 767, 472 e 347 casi. Le medesime tipologie di organizzazioni risultano essere le più prese di mira anche nel contesto italiano dove al primo posto si colloca la categoria Local Government.

# Malware la principale tecnica di attacco alle infrastrutture critiche



A livello globale, le tecniche più utilizzate per attaccare le infrastrutture critiche appartengono alle categorie Malware (36%), Unknown (27%) e Vulnerabilities (13%). Nel contesto italiano, prevale la categoria Unknown (45%), seguita da Malware (43%) e Denial of Service (4%).

# Attacchi alle infrastrutture critiche italiane: 9 su 10 causano impatti gravi o molto gravi, nessuno con impatto basso



A livello globale, il 76% degli attacchi alle infrastrutture critiche ha una severity High (47%) o Critical (29%). Nel contesto italiano, tale dato si attesta al 90%, con un 39% di attacchi con severity Critical e un 51% con severity High.



**Grazie per l'attenzione!**

**[faggioli@mip.polimi.it](mailto:faggioli@mip.polimi.it)**